

August 12, 1986

CONGRESSIONAL RECORD — HOUSE

H 6015

sense. It allows for broad classification bands, direct hiring, total compensation comparability, and pay for performance. The project will run for 5 years and be subject to rigorous evaluation each year. The Director of the National Bureau of Standards will have broad flexibility to manage the Bureau.

I think this is legislation which moves towards achieving the goal of the Civil Service Reform Act of 1978. It is worthy of our support.

Mr. BOEHLERT. Mr. Speaker, I have no further requests for time, and I yield back the balance of my time.

Mr. WALGREN. Mr. Speaker, I have no further requests for time, and I yield back the balance of my time.

The SPEAKER pro tempore (Mr. SMITH of Florida). The question is on the motion offered by the gentleman from Pennsylvania [Mr. WALGREN] that the House suspend the rules and pass the bill, H.R. 4354, as amended.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

COMPUTER SECURITY ACT OF 1986

Mr. FUQUA. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2889) to amend the act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems, as amended.

The Clerk read as follows:

H.R. 2889

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1986".

SEC. 2. PURPOSE.

(a) IN GENERAL.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.—The purposes of this Act are—

(1) to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, by amending the Act of March 3, 1901;

(2) to provide for promulgation of such standards and guidelines by amending section 111(f) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901, (15 U.S.C. 271-278h), is amended—

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof a semicolon, and by inserting after such paragraph the following:

"(2) the study of equipment, procedures, and systems for automatic acquisition, storage, manipulation, display, and transmission of information, and its use to control machinery and processes;";

(2) by redesignating section 18 as section 20, and by inserting after section 17 the following new sections:

SEC. 18. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2), of title 44, United States Code;

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce, for promulgation under section 111 of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1986; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(f) of the Fed-

eral Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(f) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1986;

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) As used in this section and section 19, the terms 'computer system', 'Federal computer system', 'operator of a Federal computer system', and 'sensitive information' have the meanings given in section 7 of the Computer Security Act of 1986.

"Sec. 19. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industry;

"(2) four members from outside the Federal Government who are eminent in fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of

H 6016

CONGRESSIONAL RECORD — HOUSE

August 12, 1986

the National Security Agency, and the appropriate Committees of the Congress.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency."; and

"(3) by adding at the end thereof the following new section:

"Sec. 21. This Act may be cited as the National Bureau of Standards Act."

SEC. 4. AMENDMENT TO BROOKS ACT.

"(a) AMENDMENT.—Section 111(f) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(f)) is amended to read as follows:

"(f)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 18(a)(2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems.

"(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by governmentwide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be promptly transmitted to the Committee on Government Operations of

the House of Representatives and the Committee on Governmental Affairs of the Senate.

"(4) The Administrator shall ensure that such standards and guidelines are implemented within an integrated information resources management system (as required by chapter 35 of title 44, United States Code) by—

"(A) developing and implementing policies on Federal computer system; and

"(B) revising the Federal information resources management regulations (41 CFR ch. 201) to implement such standards, guidelines, and policies.

"(5) As used in this section, the terms 'computer system', 'operator of a Federal computer system', and 'Federal computer system' have the meanings given in section 7 of the Computer Security Act of 1986."

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 111 of such Act is further amended—

(1) by striking out "automatic data processing equipment" and "automatic data processing systems" each place they appear and inserting in lieu thereof "computer systems"; and

(2) by striking out "Automatic data processing equipment" and inserting in lieu thereof "Computer systems".

SEC. 5. TRAINING BY OPERATORS OF FEDERAL COMPUTER SYSTEMS.

(a) IN GENERAL.—Each operator of a Federal computer system that contains sensitive information shall provide mandatory periodic training in computer security awareness and accepted computer security practice. Such training shall be provided under the guidelines developed pursuant to section 18(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section, for all employees who are involved with the management, use, or operation of computer systems.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR OPERATORS OF FEDERAL COMPUTER SYSTEM FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each operator of a Federal computer system shall identify each computer system, and system under development, of that operator which contains sensitive information. In the case of a Federal contractor or other organization (operating a Federal computer system), such identification shall be reviewed and approved by its supervising Federal agency.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such operator shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(f) of the Federal Property and Administrative Services Act of 1949, establish a plan for the se-

curity and privacy of the National computer system identified pursuant to subsection (a). Copies of such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. In the case of a Federal contractor or other organization (operating a Federal computer system), such plan shall be transmitted through its supervising Federal agency. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget.

SEC. 7. DEFINITIONS.

As used in this Act, sections 18 and 19 of the National Bureau of Standards Act, and section 111 of the Federal Property and Administrative Services Act of 1949—

(1) the term "computer system" means any equipment or interconnected collection of equipment, including—

(A) ancillary equipment;

(B) software and other procedures;

(C) services; and

(D) other resources,

that are used in the automatic acquisition, storage, manipulation, or display, or in any associated electromagnetic transmission and reception, of information;

(2) the term "Federal computer system" means a computer system operated by a Federal agency (as that term is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949) or by a contractor of a Federal agency or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal Government function;

(3) the term "operator of a Federal computer system" means a Federal agency (as that term is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949), contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal Government function;

(4) the term "sensitive information" means any information, the loss, misuse, or unauthorized access or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552 of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

SEC. 8. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to each Federal agency such sums as may be necessary for fiscal years 1987, 1988, and 1989 to carry out the computer systems security training program established by section 5 of this Act and the identification and planning requirements of section 6.

Mr. SPEAKER pro tempore. Pursuant to the rule, a second is not required on this motion.

The gentleman from Florida [Mr. FUQUA] will be recognized for 20 minutes and the gentleman from New Mexico [Mr. LUJAN] will be recognized for 20 minutes.

The Chair recognizes the gentleman from Florida [Mr. FUQUA].

GENERAL LEAVE

Mr. FUQUA. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their re-

August 12, 1986

CONGRESSIONAL RECORD — HOUSE

H 6017

marks on H.R. 2889, the bill now being considered.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Florida?

There was no objection.

Mr. FUQUA. Mr. Speaker, I yield myself 2 minutes.

Mr. Speaker, Members on both sides of the aisle have worked unusually hard on this bill. Hearings first began nearly 3 years ago in the subcommittee chaired at that time by the distinguished gentleman from Kansas [Mr. GLICKMAN]. Since then many others, including our colleagues on the Committee on Government Operations, have joined as the true size and character of the problem became clear.

□ 1240

The bill that the two committees are bringing to the floor today is a culmination of 2 year's work. It represents what I believe is a long overdue step toward solving a growing problem, one brought about by our increasing dependency on computer systems.

It is no secret that society, and especially the Government, has become highly dependent on computers and the enormous quantities of information they contain. Yet the low level of protection given this information in most cases makes it vulnerable to all kinds of abuse.

H.R. 2889 accomplishes two objectives that will lead to much stronger security of Federal computer systems. First, it calls for improved training of Federal workers in good computer security practice, and second, it provides for a strengthened focal point for developing policy and guidance for the civil agencies.

Mr. Speaker, these provisions were worked out over many months with great care, and I believe that we have a strong consensus among both committees that this bill is a practical and cost-effective approach.

Mr. Speaker, I recommend its adoption, and I reserve the balance of my time.

Mr. LUJAN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in strong opposition to this bill and really regret the need to do so. After endless hours of negotiations with my fellow colleagues, I find myself in a position where I must rise in opposition.

There are, I must say, several provisions within this bill which are meritorious and which I supported when the bill was reported out of the Committee on Science and Technology on June 4 of this year. When the Committee on Science and Technology filed the report on August 6, technical and conforming amendments were incorporated. When I raised the question as to whether these changes were in fact technical and conforming, our committee was assured by the Committee on Government Operations that in fact they were just technical and conforming. I now have serious reason, Mr.

Speaker, to believe that this advice was not accurate.

It has been brought to my attention by both the executive branch and the Committee on Armed Services of the House that section 4(b) as reported by the Committee on Science and Technology substantially expands the authority of the General Services Administration to oversee the procurement of automatic data processing equipment. In fact, there are at least three previous instances where there has been an appeal of the authority of GSA to act under the Brooks Act. As recently as May 28 of this year the Court of Appeals threw out the claim of the General Services Administration that the Government Printing Office had violated Federal procurement procedures by not operating under the Brooks Act for a contract with the Electronic Data Systems Federal Corporation [EDS] for integrated printing or publishing services for the Department of the Army.

It was the U.S. Court of Appeals for the District Court which threw out the claim that this contract represented a "Procurement under the Brooks Act * * * one conducted by authority of the General Services Administration for the acquisition of automatic data processing equipment."

Mr. Speaker, the key here is what is considered "ADP equipment." Unfortunately, I would have to agree with the Committee on Armed Services that what is now contained in the Science and Technology bill is a significant change and one that should have to be debated and voted on by the full Committee on Science and Technology.

Further, despite the fact that the chairman of the committee, the gentleman from Florida [Mr. FUQUA], offered a very reasonable solution to this dilemma, while both the Committee on Armed Services and the Republicans on the Committee on Science and Technology found it acceptable, the Committee on Government Operations could not accept it. Therefore, Mr. Speaker, what we have here is not a bill that should be on the Suspension Calendar but, rather, a very controversial bill.

The Committee on Science and Technology had made great strides in improving this legislation, and it is a travesty to view the dismantling of such substantive and committed work of the committee. Unless the amendment which the gentleman from Florida [Mr. FUQUA] offered to the Committee on Armed Services is accepted by this body by unanimous consent, the Republicans on the Committee on Science and Technology will have to oppose the bill and urge its defeat on the Suspension Calendar.

Mr. Speaker, obviously we cannot offer such an amendment, so, therefore, I must reluctantly oppose this legislation today.

Mr. FUQUA. Mr. Speaker, I yield 7 minutes to the distinguished gentle-

man from Texas [Mr. BROOKS], the chairman of the Committee on Government Operations.

(Mr. BROOKS asked and was given permission to revise and extend his remarks.)

Mr. HORTON. Mr. Speaker, will the gentleman yield?

Mr. BROOKS. I yield to the gentleman from New York.

(Mr. HORTON asked and was given permission to revise and extend his remarks.)

Mr. HORTON. Mr. Speaker, I rise in support of the bill H.R. 2889, the Computer Security Act of 1986, as reported by the Committee on Science and Technology. I am proud to have been a cosponsor of this legislation with my friend from Kansas, Mr. GLICKMAN, and others.

It is clear, as established in the hearing held on this bill by the Government Operations Committee, that the security of information gathered by the Government represents a serious problem. The GAO testified that information stored in Government computers and transmitted over connecting networks, is now vulnerable to unauthorized access and disclosure, fraudulent manipulation, and disruption. This bill establishes a system to protect this information from such misuse.

The bill directs the National Bureau of Standards to develop standards and guidelines to assure cost-effective security and privacy of sensitive information in Federal computer systems. Once these standards are established, each agency head is responsible to implement them, or more stringent ones, to protect the data within that agency deemed by the agency to be sensitive.

The bill would also require training for Federal employees in computer-security awareness, pursuant to the guidelines developed by the National Bureau of Standards.

Mr. Speaker, the Federal Government is the largest single user of computers in the world. It is estimated that by 1990, the Government will have almost one-half million microcomputers. We must act to protect the information in those computers from deliberate misuse. This bill establishes a program to do this. I support its enactment, and urge my colleagues to do likewise.

Mr. BROOKS. Mr. Speaker, as chairman of the Committee on Government Operations, I rise in full support of the Computer Security Act of 1986, H.R. 2889. I want to commend Mr. FUQUA and the other members of the Science and Technology Committee for their excellent work on the bill. Although Federal agencies have become heavily dependent on the use of computer and communication systems, little attention has been paid in the past to the protection of these systems nor the information contained in them. This is disturbing since the destruction, alteration, or manipulation

H 6018

CONGRESSIONAL RECORD — HOUSE

August 12, 1986

of these systems could undermine Federal programs and harm millions of our citizens. We cannot afford to allow this to happen.

In my view, the passage of H.R. 2889 will establish a firm statutory base to increase the awareness of computer security throughout the Federal Government. It also sets up an important research program within the National Bureau of Standards [NBS] to assess the vulnerability of Government computers and communications. It further provides for the development of technical and management technologies to defend against illegal access to sensitive agency information and for the mandatory training of Federal employees in computer and communications security.

In addition, the bill clearly delineates the roles of NBS and the National Security Agency [NSA] in the Government-wide Computer Security Program. It also establishes an advisory board to assist NBS, composed of eminent private and public sector experts in the area.

Mr. Speaker, during hearings on the bill by the Government Operations Committee, there was general agreement by all concerned that more must be done to ensure the protection of our Nation's most sensitive information. Unfortunately, the administration has decided that DOD and the National Security Agency should have virtual control over computer security throughout the entire Federal Government. Under National Security decision directive 145, DOD could control the access to not only classified information, but also to any information which it considered sensitive. Much of this information is currently located in the civilian agencies and the private sector as well. In my view, this is an unprecedented and ill-advised expansion of the military's influence into our society.

Under current law, the National Bureau of Standards has the responsibility for computer security standards. It has the expertise to fulfill this role and is the proper agency to handle this important task. I urge all Members to support the passage of the Computer Security Act of 1986, H.R. 2889.

IN OPPOSITION TO DOD ROLE IN CIVILIAN COMPUTER SECURITY

Mr. Speaker, I believe that National Security decision directive 145 is one of the most ill-advised and potentially troublesome directives ever issued by a President. It gives DOD the authority to establish regulations and standards which would govern the access to and the processing of all computerized information which it deems to be critical to the national security of the United States. This includes not only classified information but any other information within the civilian agencies which the Department considers "sensitive." I seriously question the wisdom of the President's decision to give DOD the power to classify, hence

control, information located in the civilian agencies and even the private sector which, in DOD's opinion, may affect national security.

One of the benefits of a fully and open society is the rich exchange of ideas and knowledge unfettered by governmental intervention and red-tape. The successes of our scientific, technical, and medical communities have been based upon the free exchange of data and information. Since it is a natural tendency of DOD to classify everything, it would be impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information.

NBS has just as much expertise in this area and is a far preferable place to concentrate this kind of authority. I urge all members to support H.R. 2889.

Mr. Speaker, over the last few days, DOD and OMB have gone to great lengths to create confusion and uncertainty over this legislation. It appears that they will do almost anything to defeat this measure, including making false and misleading statements regarding its provisions. For example, they have asserted that the definition of computer system in the bill greatly expands GSA's authority over computer procurements by Federal agencies.

This is simply not true. While the bill does provide, for the first time, a definition for computer system for the Brooks Act, that definition is consistent with current procurement law and regulations. It does not expand GSA's authority beyond the off-the-shelf, commercially available computer systems currently covered in GSA's implementing regulations. In fact, the definition is taken almost word for word from these regulations which have been in existence for some time.

Another assertion being made is that the bill would overturn recent court decisions regarding the Brooks Act. Once again, this is also not true. While OMB and DOD tried to convince the Federal circuit court of appeals to restrict the scope of the Brooks Act, the court, however, only ruled on a very narrow technical issue and did not accept these agencies' arguments over the scope of the act.

I urge the members to recognize the efforts of OMB and DOD for what they are—a blatant attempt to thwart this important legislation at any cost.

□ 1250

Mr. LUJAN. Mr. Speaker, I yield 4 minutes to the gentleman from California [Mr. BADHAM].

(Mr. BADHAM asked and was given permission to revise and extend his remarks.)

Mr. BADHAM. Mr. Speaker, I reluctantly rise to oppose this legislation because of my great respect for the chairman of the committee, the gentleman from Florida [Mr. FUQUA] and the chairman, the gentleman from

Texas [Mr. Brooks], whose thoughts I very greatly respect. But as a member of the Armed Services Committee I think we have gone too far on this. A lot of the information that the gentleman from Texas [Mr. Brooks] just gave us is true, and that is fine. But, if the bill does not change anything, then there is no sense having this bill, but it does do something, Mr. Speaker.

The amendments incorporated in this act before us today on suspension incorporates a definition heretofore not in the bill. The definition proposed would make the Brooks Act applicable not only to general purpose automatic data processing equipment but to all ADPE, except that which is specifically exempted under the Warner amendment.

Now, the Warner amendment was put in at the behest of DOD for the simple purpose of having computer systems that are basic to a weapons system and integrated, left out because they are unique.

This amendment would require the Department of Defense to seek procurement authority from the GSA.

Now, that is just not proper. For general purpose ADPE, OK; but for all computer equipment, software services, and other resources which might be specifically configured, but remote, rather than integral to a weapons system is absolutely wrong and should not be done.

Further, it is not clear whether the Brooks Act applies to the services to unique, as opposed to mass produced general purpose equipment, to software computer equipment used by contractors in the performance of a government contract.

DOD could no longer purchase any computer without specific approval from the GSA and that would be very destructive.

We do not object in any way the purchasing advantages of mass produced computers and general equipment, the software and the other things; but when it comes to unique computers, integral or remote, to weapons systems used for our national security for which the data must be kept classified; that is wrong.

We have tried through our staff to negotiate an agreement to remove the objectionable parts. Unfortunately, we have not been able to do that. Therefore, we must be forced to oppose this bill in its present form.

Mr. FUQUA. Mr. Chairman, I yield 6 minutes to the distinguished gentleman from Kansas [Mr. GLICKMAN].

(Mr. GLICKMAN asked and was given permission to revise and extend his remarks.)

Mr. GLICKMAN. Mr. Speaker, I rise in strong support of this bill, but let me say from the beginning, all this stuff about the DOD and the definition of computers is a side show. This is a bill which protects the records of people throughout America stored in computers. It is a bill to make sure

August 12, 1986

CONGRESSIONAL RECORD — HOUSE

H 6019

that folks who have Social Security information in Federal computers are protected so that somebody does not manipulate that data, steal it, or negligently do something with it to cause them great injury.

It is a bill that protects the veterans of America so that information which is stored in veterans computers is protected, so that folks who served in the Second World War, the Korean war, who have those records in Federal computers, those records are not manipulated. Those records are not changed.

It is a bill that does the same thing with respect to agricultural records for farmers. Those records are in AFCS computers and we want to make sure that the people who operate those computers know what they are doing to protect the information. That is the essence of this bill, and nothing in this bill, contrary to what you have heard, does anything with respect to implementing this to the defense area at all. This is a civilian bill to protect people's records in civilian computers and provide standards and organization within the National Bureau of Standards to setup that kind of information.

It is nothing but a red herring to fall victim to the logic of the Department of Defense and the Office of Management and Budget who just in the last few days have come in and said they want to kill this bill.

If you want your folks at home, the 40 or 50 million people on Social Security, the people who are veterans and the others that I have mentioned to have confidence that the information contained in Federal computers is secure, then you have to vote for this bill. That is all that it is.

Mr. FUQUA. Mr. Chairman, will the gentleman yield?

Mr. GLICKMAN. I am very happy to yield to my chairman, the gentleman from Florida.

Mr. FUQUA. Mr. Speaker, the gentleman is making a very excellent statement, and furthermore to amplify the impact, this could also apply to medical records of the VA, of the military, or the National Institutes of Health or other public health services or other types of invasions of privacy.

Mr. GLICKMAN. Mr. Speaker, the gentleman is correct.

Mr. FUQUA. Or anything with the Federal Government where records are kept.

Mr. GLICKMAN. Mr. Speaker, the gentleman is correct.

Let me just make the point here, I have a prepared statement, but I am just going to tell you a little bit about what we discovered in our hearings. We had hearings. We started where we had the 414's. Remember, they were the hackers from Milwaukee who came in and talked about how easy it was to access Federal computers. One of them accessed the computer at Los Alamos and, believe it or not, he accessed it with the same password as

was being used in the movie, "War-games." The password was "Joshua."

Then we went in and looked at other kinds of scenarios that had developed all over this country. We found that computer systems in America were a disgrace in terms of protecting them, seeing that they were viable and that people were going to lose confidence in those computer systems. They were vulnerable to manipulation, to unauthorized access. The situation was described as the electronic equivalent of leaving the bank door open.

This has great consequences for America, consequences for all those who have information stored, but also consequences for things like the operation of the air traffic control system, operation of our banking system, people coming in and destroying or manipulating records.

So what this bill does is try to improve the level of security awareness among people who use and manage Federal computers in the Federal sector. Such people are extremely important in a security sense, because studies have shown they are the greatest problem.

It is not the much publicized hacker, although I mention that to get the attention of my colleagues, working to penetrate from the outside. That is not the problem; rather, it is the insider, the one who already has access, that causes the greatest damage in practice.

We learned from the General Accounting Office, they did a survey of 25 computers in this country and they find that most of these systems have very little effort to reach the individuals to improve computer training and to make these systems less vulnerable for the purpose of enhancing security.

This bill is supposed to strengthen the link. It establishes a research program at the National Bureau of Standards aimed at developing guidance for the use by agencies, civil agencies, in structuring computer systems awareness training programs for their employees.

It also requires that such training be given periodically in each agency.

It establishes a focal point in the Government for developing computer security system standards to protect unclassified, but sensitive information.

The evidence is clear. We have thousands and thousands of Government computers at regional offices, at decentralized institutions and in Washington. We have all of America's personal records stored on these computers. They must be protected better than they are. That is the purpose of this bill.

It does nothing with the Department of Defense weapons system. It is a civilian bill, totally, completely and 100 percent. It was never referred to the Armed Services Committee because it does not deal at all with the Department of Defense in terms of a military-related function. That is red herring.

So in closing, before I yield, I will say again that if those of my colleagues have constituents who have records stored in Federal computers, you want to make sure those people believe those records are secure, they are safe, cannot be manipulated, cannot be stolen, cannot be taken and sent to some direct mail firm, cannot be used to reduce their benefits from the Government, that is the purpose of this bill. That is why I think you ought to vote for it.

Mr. LUJAN. Mr. Speaker, will the gentleman yield?

Mr. GLICKMAN. I yield to the gentleman from New Mexico.

Mr. LUJAN. Mr. Speaker, I think what the gentleman is saying is absolutely correct and I would not disagree with one word the gentleman has said, except for one thing. When we walked in here, figuratively, we were all in support of this legislation because we recognized that the things the gentleman is talking about needed to be done to protect that information.

What made us turn around and oppose the legislation is that after it left the committee, there was a little section included in there that was called "technical and conforming amendments," and I put that in quotes because what that did, it expanded the application of the Brooks amendment to the Department of Defense. It is only that on page 12, lines 14 through 22, that we are objecting to.

The SPEAKER pro tempore (Mr. WHITLEY). The time of the gentleman from Kansas has expired.

Mr. LUJAN. Mr. Speaker, I yield 1 additional minute to the gentleman from Kansas.

Mr. GLICKMAN. Well, first of all, Mr. Speaker, I would like to say that this agreement has been reached for some time and when the gentleman was supporting the combined bill, even with the language to which he referred to today, somebody had been calling the Office of Management and Budget or the Department of Defense, they have never liked this bill. Why? Because DOD wants to control all security in the United States. They do not want to give any of this control and supervision to the civilian agencies of Government; but I would be glad to yield to my colleague, the gentleman from Texas [Mr. Brooks] again to respond, as he did before, on this issue of the language that the gentleman from New Mexico referred to.

Mr. BROOKS. Mr. Speaker, if the gentleman will yield, I will be delighted to state again that this does not expand the Brooks Act. It does not expand the authority of the GSA. The Defense Department will still be operating under the Warner provisions. Everything that moves, shakes, flies, digs, shoots, crawls, hops, skips, that has a computer in it that the Defense Department has got the money for and has built is all exempted now, has been and will be.

H 6020

CONGRESSIONAL RECORD — HOUSE

August 12, 1986

□ 1305

Mr. LUJAN. Mr. Speaker, I yield 3 minutes to the gentleman from Arizona [Mr. STUMP].

Mr. STUMP. I thank the gentleman for yielding time to me.

Mr. Speaker, I rise in opposition to H.R. 2889, the Computer Security Act of 1986. Its enactment would increase—not decrease—the obstacles to computer security. The President's computer security initiative capitalizes on the unique expertise already available at the National Security Agency for Government-wide support to computer security improvement efforts. In contrast, H.R. 2889 splits up the computer security function between two agencies—NSA and the National Bureau of Standards—resulting in inefficiency, unnecessary duplication, and waste of taxpayers' dollars.

The bill contributes nothing toward improving our national security. It just increases Government redtape. I urge my colleagues to vote against H.R. 2889.

Mr. FUQUA. Mr. Speaker, I yield 2 minutes to the gentleman from Pennsylvania [Mr. WALGREN].

Mr. WALGREN. Mr. Speaker, I rise in support of this bill as it has developed in the Committees on Science and Technology and Government Operations.

I would like to emphasize the points made by the gentleman from Kansas [Mr. GLICKMAN] of the pervasiveness of computers in our society. We rely on them for literally the most basic of functions. The Federal Government has 17,000 medium- and large-scale computers, and in the immediate future is estimated to have something in the range of 500,000 microcomputers.

It is absolutely essential, considering the kind of use that these machines will be put to, that we have basic standards covering their security, and also that we have real sensitivity in the personnel that are involved in their operation, if the American public is to have any sense of private individual range and difference between Government and the individual.

These computers are involved in the most sensitive things from keeping aircraft from colliding to, as the gentleman from Kansas says, the banking system, the payment out of entitlements in the billions-of-dollars range. This is a small bill that can save literally billions and billions of dollars' worth of mistakes in our Government in areas that should not be the province of the military, and should not be the province of any national security agency.

The bill walks a good line. It should have a broad base of support, and I urge all my colleagues to support the bill.

Mr. LUJAN. Mr. Speaker, I yield 3 minutes to the gentleman from Wyoming [Mr. CHENEY].

Mr. CHENEY. Mr. Speaker, I rise in opposition to H.R. 2889. I think that

the goals and objectives of the bill are commendable. I do not quarrel at all with the objectives laid out by the gentlemen from Florida, Texas, or Kansas. I think that all of us are deeply concerned about the problem of computer security, but this was not an original thought with our friends on Government Ops or Science and Technology. It is an issue that has been addressed for a long time by many of us on the Intelligence Committee and the Armed Services Committee.

There has been a great deal of work already undertaken, a lot of money spent, and a lot of time and effort devoted to the notion that we need to make secure our computer capabilities. That expertise now resides in the NSA and the Department of Defense.

Many of us, I think, would be prepared to work with our friends on the other committees to try to perfect the legislation to make certain that it did not, in fact, create the kinds of overlapping jurisdictions and responsibilities that the gentleman from Arizona [Mr. STUMP] mentioned.

Unfortunately, Mr. Speaker, the procedure that we are following here today does not permit that. The bill is brought up under suspension of the rules. We are not able to amend it, we are not able to perfect it, and we are not able to work to try to improve it to make certain that what is being done on the domestic side does not conflict with what is being done on the national security side.

Finally, Mr. Speaker, the administration has made very clear its opposition to this legislation. The Under Secretary of Commerce, Mr. Brown, a distinguished former member of this committee, speaking for the Department, has argued against its passage. The Secretary of Defense has argued against its passage. Finally, the President's senior advisers has indicated that if this bill were to reach the President's desk in its present form, they would recommend its disapproval.

So I would urge my colleagues, Mr. Speaker, to defeat the motion that is before us today, and to bring the bill up under some other form that will give us the opportunity to perfect it, to work to see to it that we can achieve the objectives of those of us who are concerned about computer security, which I think is a goal that many of us share.

Mr. LUJAN. Mr. Speaker, I yield 4 minutes to the gentleman from Oklahoma [Mr. McCURDY].

(Mr. McCURDY asked and was given permission to revise and extend his remarks.)

Mr. McCURDY. Mr. Speaker, I rise in opposition to H.R. 2889, and I do so with some reluctance from the standpoint that as a member of the Committee on Science and Technology, in addition to Armed Services and Intelligence, it has been a rare occasion in the nearly 6 years that I have served

with the chairman, the gentleman from Florida [Mr. FUQUA], that I have had strong disagreement with or opposed any of his pieces of legislation. But I do so today because I believe that the bill goes far beyond the original intent of its author, the gentleman from Kansas [Mr. GLICKMAN], and, I believe, is an unwise step for us to take, especially on this Suspension Calendar.

Mr. Speaker, this bill calls for the establishment of a second center for computer security within the U.S. Government. We don't need a second center. The one already established is doing a good job under the supervision of the National Security Agency. I support computer security standards, and I support the research. I just question the creation of a second bureaucracy to perform the same function.

Originally set up by direction of the President under NSDD 145, as the Department of Defense Computer Security Center, it was expanded 10 months ago to become the National Computer Security Center, and, as such, is serving the entire Government's computer security needs.

By calling for a second computer security center, run and supervised by the National Bureau of Standards, this bill would require the taxpayers to pay twice the bureaucratic overhead costs associated with computer security. The National Security Agency already possesses the special expertise required for the computer security discipline and has applied it effectively in its computer security role under NSDD 145. No such expertise currently resides in the National Bureau of Standards and it would take considerable time and additional cost for such expertise to be developed.

The National Security Agency has already spent significant sums to develop the capability to handle all aspects of computer security. It doesn't take much sense to take a mission away from an organization that has developed the expertise and has the best equipment to handle this critical problem. Furthermore, this bill will force businesses dealing with the Federal Government to adjust their computer activities to accommodate the computer security requirements of two Federal Government organizations, thus resulting in increased costs and twice as much redtape with no greater quality of computer security.

Computer security science is very challenging and, to do it right, it must be done with the best expertise, and by the most highly motivated people. The National Security Agency has already expended significant time, effort, and money, to develop the capability to handle all aspects of computer security. A lot of this would be wasted if NSA was responsible only for computer security for classified information.

August 12, 1986

CONGRESSIONAL RECORD — HOUSE

H 6021

From my personal observation as a member of the Intelligence Committee, I am convinced that the National Security Agency is highly dedicated and motivated to insure the availability of first-rate computer security for the entire Government. Let me point out that the entire executive branch opposes this bill—to include those agencies most directly involved, the Department of Defense, the National Security Agency, the Office of Management and Budget, and even the Department of Commerce, which has the supervisory authority over the National Bureau of Standards. Deputy Secretary of Commerce, Clarence J. Brown, has stated that the creation of such a center in the National Bureau of Standards would “impose totally inappropriate tasks on the National Bureau of Standards.”

Let me address the real bottom line of this bill. Proponents of this bill state that, by allowing the National Security Agency to have a role in computer security outside the military and intelligence arena, it might tempt the NSA to conduct domestic surveillance activities in violation of its charter. In my opinion, that is the real red herring in this debate. This acquisition totally ignores the development over the last 10 years of detailed legal controls on the intelligence community, to include the National Security Agency, and of the close scrutiny of the National Security Agency by the House and Senate Intelligence Committees. In sum, we don't need to set up a duplicative center in order to prevent potential violations of the NSA Charter. With the oversight process in the Intelligence Committees we have the mechanism to prevent such abuses from occurring.

Mr. Chairman, let me reiterate my opposition to this bill and I ask for a recorded vote on H.R. 2889.

□ 1315

Mr. GLICKMAN. Mr. Speaker, will the gentleman yield?

Mr. McCURDY. I yield to the gentleman from Kansas.

Mr. GLICKMAN. Mr. Speaker, I guess the main concern is that do you want to give NSA, a military agency, exclusive and complete authority over civilian agencies like the Social Security Administration, the Veterans' Administration in terms of computer security standards. I think that is a philosophical issue. I think it is a mistake myself.

Mr. FUQUA. Mr. Speaker, which member gets to close debate?

The SPEAKER pro tempore. The gentleman from Florida [Mr. FUQUA] has the right to close the debate.

Mr. FUQUA. Mr. Speaker, I reserve the balance of my time.

Mr. LUJAN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I simply would like to make one closing point.

It has been said that this technical and conforming amendment, does not

do anything, does not expand the authority of the Brooks Act. I might say that if we could remove that we would be supportive of the bill. However, with that item in there, I do not think that we could.

That is why we would oppose it, but only on suspension. That would give us an opportunity if we got a rule to be able to offer an amendment to change it.

Mr. VOLKMER. Mr. Speaker, will the gentleman yield?

Mr. LUJAN. I yield to the gentleman from Missouri.

Mr. VOLKMER. I thank the gentleman for yielding. I too agree with the gentleman that this language on page 12, lines 14 on down, needs to be deleted. I believe we all should have an opportunity on the floor to offer an amendment to do that, and that we should not vote for the bill on suspension.

Mr. LUJAN. The gentleman is absolutely correct. He and I both sit on the Committee on Science and Technology, and it was not until afterward that we found, in consultation among the staffs, that this wording had been put in there.

So, reluctantly, Mr. Speaker, we must oppose it.

Mr. FUQUA. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I think we have received the assurances of the gentleman from Texas [Mr. Brooks], chairman of the Committee on Government Operations and the author of the Brooks Act, so named for him, that this does not expand authority currently granted.

In looking on page 15 at the definition of the issue just raised about computer systems, it defines those issues “ancillary equipment, software and other procedures, services, and other resources.”

When you look at the regulations that are already in effect, this is somewhat more narrow than the regulations. So I think this is not a valid argument that this totally and broadly expands.

It was stated by the gentleman from Texas [Mr. Brooks] that that was not the intention, and it did not, in fact, do that. It does not overturn court cases that have now or may be pending, and that is not the intent of the legislation.

As the gentleman from Kansas pointed out, what we are trying to do is establish within a civilian agency, the National Bureau of Standards, the means to help develop standards for nonclassified information of the Federal Government. We are not trying to get into the DOD. We are not trying to get into the National Security Agency or the CIA or other agencies of that type.

The question involves who knows the most about computers. The National Bureau of Standards is recognized as one of the world authorities on computers and computer standards.

They are already involved in that type of information and that type of work, and have some very distinguished people working in the Bureau of Standards to carry out those programs.

I would plead with my colleagues that the one issue we are involved with is not DOD or the security agency. That is a smokescreen, and that is not what we are trying to do. Neither does the bill do that.

What we are trying to do is establish within a civilian agency the standards that can be used in order to make more secure the computer systems that we have that contain nonclassified information, such as the Social Security information, such as Veterans' Administration information, such as IRS information, and other types of information that have been outlined here on the floor.

I urge Members not to be misled by some of the stories, and the horror stories that have been presented by the OMB. They have not supported the bill from the beginning, and they have fought it every inch of the way. We have tried to accommodate every objection they have raised. Unfortunately, Mr. Speaker, they have raised more objections each step we go along, and throw out more barriers. It is almost like hurdles in a race.

So I would urge the Members not to be bamboozled by some of the smoke-screens and the stories that have been raised by OMB, and to support a bill for civilian control for nonclassified information.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. WHITLEY). The question is on the motion offered by the gentleman from Florida [Mr. FUQUA] that the House suspend the rules and pass the bill, H.R. 2889, as amended.

The question was taken; and on a division (demanded by Mr. LUJAN) there were—yeas 5, nays 14.

Mr. FUQUA. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to the provisions of clause 5, rule I, and the Chair's prior announcement, further proceedings on this motion will be postponed.

The point of no quorum is considered withdrawn.

TECHNOLOGY EDUCATION ACT OF 1985

Mr. BOUCHER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3102) to strengthen the technological literacy of the Nation through demonstration programs of technology education, as amended.

The Clerk read as follows:

H 6022

CONGRESSIONAL RECORD — HOUSE

August 12, 1986

H.R. 3102

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Technology Education Act of 1986".

SEC. 2. FINDINGS AND PURPOSES.

It is the purpose of this Act to assist educational agencies and institutions in developing a technologically literate population through instructional programs in technology education.

SEC. 3. DEFINITIONS.

For the purposes of this Act—

(1) the term "technology education" means a comprehensive educational process designed to develop a population that is knowledgeable about technology, its evolution, systems, techniques, utilization in industry and other fields, and social and cultural significance;

(2) the term "local educational agency" has the meaning given such term in section 198(a)(10) of the Elementary and Secondary Education Act of 1965;

(3) the term "State educational agency" has the meaning given such term in section 198(a)(17) of the Elementary and Secondary Education Act of 1965;

(4) the term "institution of higher education" has the meaning given such term in section 1201(a) of the Higher Education Act of 1965; and

(5) the term "Secretary" means the Secretary of Education.

SEC. 4. TECHNOLOGY EDUCATION DEMONSTRATION PROGRAM.

(a) **ESTABLISHMENT.**—Subject to the availability of funds for purposes of this Act, the Secretary of Education shall establish a program of grants to local educational agencies, State educational agencies, consortia of public and private agencies, organizations and institutions, and institutions of higher education to establish not more than ten demonstration programs in technology education for secondary schools.

(b) APPLICATION.—

(1) A local educational agency, State educational agency, consortium of public and private agencies, organizations, and institutions, or institution of higher education which desires to receive a grant under this Act shall submit an application to the Secretary. Applications shall be submitted at such time, in such form, and containing such information as the Secretary shall prescribe and may be approved only if such application—

(A) describes a demonstration program for carrying out the purposes under subsection (c);

(B) contains an estimate of the cost for the establishment and operation of the program;

(C) sets forth such policies and procedures as will ensure adequate evaluation of the activities intended to be carried out under the application;

(D) contains assurances that Federal funds made available under this Act will be so used as to supplement and, to the extent practicable, increase the amount of State and local funds that would in the absence of such Federal funds be made available for the uses specified in this Act, and in no case supplant such State or local funds;

(E) provides for making such reports, in such form and containing such information, as the Secretary may reasonably require; and

(F) describes the manner in which programs under this Act will be coordinated, to the extent practicable, with programs under the Job Training Partnership Act, the Carl D. Perkins Vocational Education Act, and

other Acts related to the purposes of this Act.

(2) Amendments of applications shall be subject to approval in the same manner as original applications.

(3) In making grants under this Act the Secretary shall consider the equitable geographic distribution of such grants.

(c) **USES OF FUNDS.**—Funds made available under this Act may be used to develop a model demonstration program for technology education with the following components:

(1) Educational course content based on—
(A) an organized set of concepts, processes, and systems that is uniquely technological; and

(B) fundamental knowledge about the development of technology and its effect on people, the environment, and culture.

(2) Instructional content drawn from introduction to technology education courses in one or more of the following areas:

(a) communication—efficiently using resources to transfer information to extend human potential;

(b) construction—efficiently using resources to build structures on a site;

(c) manufacturing—efficiently using resources to extract and convert raw or recycled materials into industrial and consumer goods; and

(d) transportation—efficiently using resources to obtain time and place utility and to attain and maintain direct physical contact and exchange among individuals and societal units through the movement of materials, goods, and people.

(3) Assisting students in developing insight, understanding, and application of technological concepts, processes, and systems.

(4) Educating students in the safe and efficient utilization of tools, materials, machines, processes, and technical concepts.

(5) Developing student skills, creative abilities, confidence, and individual potential in utilizing technology.

(6) Developing student problem-solving and decision-making abilities involving human and material resources, processes, and technological systems.

(7) Preparing students for lifelong learning in a technological society.

(8) Activity-oriented laboratory instruction which reinforces abstract concepts with concrete experiences.

(9) An institute for the purposes of developing teacher capability in the area of technology education.

(10) Research and development of curriculum materials for use in technology education programs.

(11) Multi-disciplinary teacher workshops for the interfacing of mathematics, science, and technology education.

(12) Statewide implementation plan for disseminating exemplary materials and practices.

(13) Optional employment of a curriculum specialist to provide technical assistance for the program.

(14) A combined emphasis on "know-how" and "ability-to-do" in carrying out technological work.

(d) **LIMITATION ON FEDERAL ASSISTANCE.**—Federal assistance to any program or project under this Act shall not exceed 65 percent of the cost of such program in any fiscal year. Not less than 10 percent of the cost of such program shall be in the form of private sector contributions. Non-Federal contributions may be in cash or in kind, fairly evaluated, including facilities, overhead, personnel, and equipment.

(e) **NATIONAL DISSEMINATION OF INFORMATION.**—The Secretary shall disseminate the results of the programs and projects assist-

ed under this Act in a manner designed to improve the training of teachers, other instructional personnel, counselors, and administrators.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

(a) **FUNDING UNDER SECRETARY'S DISCRETIONARY FUNDS.**—For each of the fiscal years 1987, 1988, and 1989, of the funds appropriated to carry out the Secretary's Discretionary Funds under section 583 of the Education Consolidation and Improvement Act of 1981 \$2,000,000 shall be available to carry out the provisions of this Act.

(b) **AMENDMENT TO ECIA.**—Section 583 of the Education Consolidation and Improvement Act of 1981 is amended by adding the following subsection:

"(c) For each of the fiscal year 1987, 1988, and 1989, from the funds reserved for the purposes of this section, subject to the provisions of subsection (b), the Secretary shall make available \$2,000,000 to carry out the Technology Education Act of 1986."

SEC. 6. EFFECTIVE DATE.

The provisions of this Act shall take effect October 1, 1986.

The SPEAKER pro tempore. (Mr. SMITH of Florida). Is a second demanded?

Mr. GOODLING. Mr. Speaker, I demand a second.

The SPEAKER pro tempore. Without objection, a second will be considered as ordered.

There was no objection.

The SPEAKER pro tempore. The gentleman from Virginia [Mr. BOUCHER] will be recognized for 20 minutes and the gentleman from Pennsylvania [Mr. GOODLING] will be recognized for 20 minutes.

The Chair recognizes the gentleman from Virginia [Mr. BOUCHER].

Mr. BOUCHER. Mr. Speaker, I yield myself such time as I may consume.

(Mr. BOUCHER asked and was given permission to revise and extend his remarks.)

Mr. BOUCHER. Mr. Speaker, I would like to thank the distinguished chairman of the Education and Labor Committee, Mr. HAWKINS, for his support and assistance in bringing this measure to the floor. I would also like to thank the gentleman from Pennsylvania [Mr. GOODLING] for his assistance in crafting a bill that will encourage the development and implementation of technology education demonstration projects.

The Technology Education Act recognizes the need for a population that is knowledgeable about the historical development and current application of technology. During the past century, we have witnessed a dramatic change in our Nation's economic base. Information and services have replaced agriculture and manufacturing as the growth sectors of the U.S. economy.

We led the world in the technological revolution through the development of electronics, the internal combustion engine and a host of other inventions. Now, however, our international competitors are gaining preeminence in the technical fields we pioneered.